48 36
~~73~~. The computer system as recited in claim ~~38~~, wherein the mechanism indirectly identifies the encryption method.

REMARKS

In the final Office Action, the Examiner rejected the claims under 35 USC § 251, 35 USC §112 and under 35 USC §102. These objections and rejections are fully traversed below.

The claims have been amended to correct minor informalities and to further clarify the subject matter regarded as the invention. Claims 1-73 remain pending.

Reconsideration of the application is respectfully requested based on the following remarks.

REJECTION OF CLAIMS 26-53 UNDER 35 USC §251

In the Office Action, the Examiner rejected claims 40-53 and 60-68 under 35 USC §251 as being an improper recapture of claimed subject matter cancelled in the application for the patent upon which the present reissue is based. As pointed out by the Examiner, original claims 6 and 14 were amended to specifically require that a new header be generated when the data packet is encrypted. As is understood by the Examiner, original claims 6 and 14 were directed at encryption of the data packet while the rejected claims 40-53 and 60-68 are directed to decryption rather than encryption. The Examiner has taken the position that since decryption is the complementary process to encryption, "the decryption process claimed must contain the second header as well" to avoid recapturing the material implicitly. Therefore, the Examiner has implied that the encryption process requires the generation of a **second header**.

Generation of a new address header does not require or imply that a second header is generated during encryption. The amendments to original claims 6 and 14 during prosecution of the original patent do not recite a second header. Moreover, although it is possible that the new header is a second header that is appended to the data packet, the new header may also merely be a replacement header to an already existing header to the data packet. The only requirement

imposed by the amendments to original claims 6 and 14 is that a new header be generated and appended to the data packet.

The first step in applying the recapture rule is to determine whether and in what aspect the reissue claims are broader than the patent claims. As discussed above, the encryption step does not require that a second header be generated. Therefore, the fact that the decryption step does not recite a second header does not broaden the reissue claims in this respect. It follows that application of the second step in which it is determined whether the broader aspects of the reissue claims relate to surrendered subject matter becomes moot. Accordingly, the absence of the recitation of a second header in the decryption step does not "recapture" claimed subject matter surrendered in the application to obtain the original patent.

Specifically, claims 40-53 and 60-68 do recite a header. More particular, as described above, each of claims 40-53 and 60-68 recite receiving a data packet including a header section and a data section. The feature they do not recite is where the header is generated. It is acknowledged that in many (and probably most) situations, the header that is on the decrypted packet will have been generated by the encryption source. However, this is by no means a requirement. It is well known in the networking arts that there are a number of devices which strip a header and append a new header without affecting the data packet. For example, it is easy to contemplate a situation where a first node encrypts the data packet and appends an appropriate header to the encrypted data packet. The encrypted data packet is then forwarded to a second node which strips the header appended by the first node and appends its own header. From the standpoint of the device handling the encryption, it may be quite irrelevant which process or mechanism appended the header to the data packet that is being decrypted. Thus, in the present case, the encryption and decryption are NOT necessarily mirror images of one another. Accordingly, it is respectfully submitted that amendments made to the encryption claims do not have an estoppel effect on the claims directed at decryption, and that the pending rejection of claims 40-53 and 60-68 under 35 USC §251 should be reversed.

REJECTION OF CLAIMS UNDER 35 USC §112

In the Advisory Action, the Examiner indicated that claims 1, 11, and 18 continue to be rejected under 35 USC §112, second paragraph, as being indefinite for failing to particularly

point out and distinctly claim the subject matter which Applicant regards as the invention. However, claims 1 and 11 already conform to the Examiner's recommendations. With reference to claim 18, decryption of the packet may include decryption of the header of the data packet as well as the body of the data packet. Thus, the claim has been amended to perform decryption of at least a portion of the data packet. Hence, Applicant respectfully requests that the Examiner withdraw the rejection of the claims under 35 USC §112, second paragraph.

REJECTION OF CLAIMS UNDER 35 USC §102

White

Claims 32-33, 40-41, and 44-53 stand rejected under 35 USC §102(b) as being anticipated by White. In the Office Actions, the Examiner has argued that the Site Address (for entry into the WAN) disclosed in White is a network address which is the same as the "broadcast address" as defined in Applicant's specification. Applicant respectfully traverses this assertion. Col. 4, lines 10-15 of White state that the header contains Site Address information that identifies a **node** via which the packet enters and leaves the WAN. Thus, the Site Address disclosed in White refers to a specific node rather than a "broadcast address," as will be described in further detail below.

Independent claims 40, 50, and 52

Each of independent claims 40, 50, and 52 pertain to a method, a computer program product, or a computer system for decryption of a data packet including a header section that stores a destination identifier of a broadcast address of the destination of the data packet and a source identifier of a broadcast address of the source of the data packet.

Applicant acknowledges that White discloses a header that identifies the node via which the packet enters and leaves the network (i.e., Site Address). See White, col. 4, lines 11-15. However, Applicant respectfully submits that the Site Address disclosed in White is not equivalent to a broadcast address. Claims 40, 50, and 52 each specifically require that the header

section store a source identifier identifying a "broadcast address" of the source and a destination identifier identifying a "broadcast address" of the destination. The term "broadcast address" is known in the art to refer to an IP address used for transmitting packets to all hosts on a given network. In other words, through the use of a broadcast address, a single host cannot be identified. In practice, the host portion of a broadcast address typically contains all 1s or all 0s. White neither discloses nor suggests that the header identifies a *broadcast* address of the source and destination of the data packet. Rather, White requires that the header identify an actual node via which the packet enters and leaves the network, as described above. The invention of claims 40, 50, and 52 prevents using the address of a particular node, particularly a node responsible for encryption or decryption of the data packet. The presently claimed invention therefore provides greater protection against tapping into the network to decipher the nature of the information transmitted. Accordingly, Applicant respectfully submits that White's disclosure of a header that identifies a node via which a packet enters and leaves a network does not anticipate claims requiring that a header section of a data packet include a source identifier identifying a "broadcast address" of the source and a destination identifier identifying a "broadcast address" of the destination.

Each of claims 40, 50, and 52 further require determining whether the data packet is encrypted upon reference to at least one of the source and destination identifiers and decrypting the data packet to produce a decrypted data packet if the data packet is encrypted. White neither discloses nor suggests determining whether a data packet is encrypted upon reference to at least one of the source and destination identifiers, which identify a "broadcast address" of the source and a "broadcast address" of the destination, respectively. Nor does White disclose or suggest decrypting the data packet upon such a determination. Therefore, it is respectively submitted that claims 40, 50, and 52 are not anticipated by White, and that the pending rejection of these claims should be reversed for the reasons set forth.

Dependent claims 41, 44-49, 51, and 53

Claim 41 depends directly from independent claim 40 and further comprises transmitting the decrypted data packet to the destination. Applicant respectfully submits that White neither

discloses nor suggests transmitting a decrypted data packet to a destination which has been decrypted upon a determination made as described above with reference to claim 40. Accordingly, claim 40 is not anticipated by White and the pending rejection of claim 40 should be reversed for this reason as well.

Claim 44 depends directly from independent claim 40 and further requires that the data section of the data packet include an encrypted header section and an encrypted data section, the encrypted header section including a header of the decrypted data packet after encryption and the encrypted data section including a body of the decrypted data packet after encryption. White neither discloses nor suggests such an encrypted header section and encrypted data section. Thus, Applicant respectfully submits that claim 44 is patentable over White, and respectfully requests that the rejection of claim 44 be reversed for this reason as well.

Claims 45-47 further depend from claim 44. Claim 45 depends from claim 44 and further recites wherein the encrypted header section stores the source and destination identifiers. White neither discloses nor suggests storing the source and destination identifiers (which identify broadcast addresses of the source and destination, respectively) in an encrypted header section. Thus, Applicant respectfully submits that claim 45 is not anticipated by White, and respectfully submits that the rejection of claim 45 should be reversed for this reason as well.

Claim 46 depends from claim 44 and further recites wherein the source is a network and the encrypted header section stores an identifier of a host computer in the network. White neither discloses nor suggests storing an identifier of a host computer in the network (which is the source of the packet) in an encrypted header. Thus, Applicant respectfully submits that claim 46 is not anticipated by White, and respectfully submits that the rejection of claim 46 should be reversed for this reason as well.

Claim 47 depends from claim 44 and further recites wherein the destination is a network and the encrypted header section stores an identifier of a host computer in the network. White neither discloses nor suggests storing an identifier of a host computer in the network (which is the destination of the packet) in an encrypted header. Thus, Applicant respectfully submits that claim 47 is not anticipated by White, and respectfully submits that the rejection of claim 47 should be reversed for this reason as well.

Claim 48 depends from claim 40 and further requires that the source is a host computer or a network. White neither discloses nor suggests performing the method of claim 40 where the source is a host computer or a network. Thus, Applicant respectfully submits that claim 48 is not anticipated by White, and respectfully submits that the rejection of claim 48 should be reversed for this reason as well.

Claim 49 depends from claim 40 and further requires that the destination is a host computer or a network. White neither discloses nor suggests performing the method of claim 40 where the destination is a host computer or a network. Thus, Applicant respectfully submits that claim 49 is not anticipated by White, and respectfully submits that the rejection of claim 49 should be reversed for this reason as well.

Claim 51 depends from claim 50 and further requires that the computer readable medium is a memory, random-access-memory, read-only-memory, disk drive, or CD-ROM. White neither discloses nor suggests storing the computer program product of claim 50 in such a computer readable medium. Accordingly, Applicant respectfully submits that claim 51 is not anticipated by White, and respectfully submits that the rejection of claim 51 should be reversed for this reason as well.

Independent claims 32 and 33

Claim 32 pertains to a method of encryption that produces a modified data packet including a header portion that stores an identifier of the network of the source of the data packet. Similarly, claim 33 pertains to a method of encryption that produces a modified data packet including a header portion that stores an identifier of the network of the destination of the data packet. Thus, both claims 32 and 33 each specifically require that an identifier of a network be provided in a header portion of the data packet.

A single host cannot be identified through the mere identification of a network. As described above, White requires that the header identify an actual node via which the packet enters and leaves the network, as described above. In contrast, the invention of claims 32 and 33 prevents using the address of a particular node, particularly a node responsible for encryption or decryption of the data packet. The presently claimed invention therefore provides greater protection against tapping into the network to decipher the nature of the information transmitted. Accordingly, Applicant respectfully submits that White's disclosure of a header that identifies a node via which a packet enters and leaves a network does not anticipate claims requiring that a header section of a data packet include an identifier of a network of the destination or source of the data packet. Therefore, it is respectively submitted that claims 32 and 33 are not anticipated by White, and that the pending rejection of these claims should be reversed for the reasons set forth.

Adams, Jr. – claims 7-8, 14-15, 18-19, 21-23, 32-33, 40-53, and 56-59

Claims 7-8, 14-15, 18-19, 21-23, 32-33, 40-53, and 56-59 stand rejected as being anticipated by Adams, Jr. et al. Adams Jr. discloses a computer network encryption/decryption device (CNEDD) that operates in one of two modes by selectively encrypting or decrypting packets based on information contained in a packet's header. See Adams, Jr., Abstract. When the CNEDD operates in the standard mode, only the data portion of a packet is encrypted, and a new packet is transmitted which includes an unencrypted header (with the original routing information) and the encrypted data. See Adams, Jr., col. 6, lines 63-68. In the tunneling mode, both the data characters and the header characters of a packet are encrypted. See Adams, Jr., col. 6, line 68 – col. 7, line 2. In addition, encryption and decryption is performed based on information contained in a table, as described in Adams. See Adams, Jr., col. 7, lines 17-41. Rather than including the routing information from the original data packet in the header of the encrypted packet, the header indicates that the source of the packet is a CNEDD and the destination of the packet is a CNEDD in the network which contains the intended target node. See Adams, Jr., col. 9, line 57 – col. 10, line 2. In his rejections, the Examiner has stated that the CNEDD address is a network address and that the gateway (CNEDD) address is used in the new header. The Examiner has essentially asserted that the specification of the CNEDD address in a packet header is somehow equivalent to the rejected claims which identify broadcast addresses or networks associated with the source and/or destination of the packet in a packet header. Applicant respectfully traverses this assertion.

Independent claim 7

Claims 7 is drawn to a system for encrypting and decrypting data packets, in which a new address header including internetwork broadcast addresses of the first and second computer networks (corresponding to the source and destination of the data packet) is appended to the data packet when the data packet is encrypted.

Adams, Jr., like White, discloses the specification of an address of a particular node in the packet header. Adams, Jr. specifically requires that the gateway (CNEDD) address is be provided in the packet header. In contrast, the invention of claim 7 specifically provides broadcast addresses of the source and destination in the packet header. In this manner, the present invention avoids providing the address of a gateway responsible for encryption and/or decryption of the data packet in the packet header, as disclosed by Adams, Jr. The system in

Adams, Jr. is entirely susceptible to outsiders wishing to tap into the network, since such outsiders may easily ascertain the nodes responsible for encryption as well as decryption. The presently claimed invention therefore provides greater protection than Adams, Jr. against tapping into the network to decipher the nature of the information transmitted (e.g., via the gateway responsible for encryption or decryption).

Claim 7 further recites "a first table stored in said first memory including a correlation of at least one of the first host computer and the first network with one of the second host computer and the second network, respectively" and instructions for "determining whether said correlation is present in said first table, and if so, then executing encryption of said first data packet." Similarly, claim 7 further recites "a second table stored in said second memory including a correlation of at least one of the first host computer and the first network with one of the second host computer and the second network, respectively" and instructions for "determining whether said correlation is present in said second table, and if so, then executing decryption of said first data packet." Thus, correlations may exist between the source and destination computers via the associated networks. In this manner, the information provided in the packet header (i.e., the broadcast addresses) may be used to determine whether a packet is to be encrypted as well as whether a packet is to be decrypted. Adams, Jr. neither discloses nor suggests the use of such tables to perform encryption or decryption. Applicant therefore respectfully submits that claim 7 is not anticipated by Adams, Jr., and that the pending rejection of claim 7 should be reversed for at least the reasons set forth.

Dependent claim 8

Claims 8 depends directly from independent claim 7. Claim 8 further requires that the new address header include an identifier of the second bridge computer. Adams, Jr. does not disclose the system of claim 7 and further include an identifier of the second bridge computer in the packet header. Applicant therefore respectfully submits that claim 8 is not anticipated by Adams, Jr., and that the pending rejection of claim 8 should be reversed for this reason as well.

Independent claim 14

Claim 14 is drawn to a system for encrypting and decrypting data packets, in which a new address header is generated and appended to the data packet when the data packet is encrypted, where the new address header identifies broadcast addresses of the first and second computer networks (corresponding to the source and destination of the data packet).

As described above, Adams, Jr. specifically requires that the gateway (CNEDD) address be provided in the packet header. This gateway address is in no manner equivalent to a broadcast address. It is therefore respectfully submitted that claim 14 is not anticipated by Adams, Jr., and that the pending rejection of claim 14 should be reversed for this reason as well.

Dependent claims 15 and 56

Claim 15 depends from claim 14 and further recites correlation data identifying at least one of said first host computer and said first network correlated with at least one of said second host computer and said second network. In addition, a determination whether to encrypt data packets is performed by inspecting for a match between source and destination addresses of said data packets with said correlation data. Thus, correlation data may define correlations between the source and destination computers via the associated networks. In this manner, the information provided in the packet header (i.e., the broadcast addresses) may be used to determine whether a packet is to be encrypted as well as whether a packet is to be decrypted. Adams, Jr. neither discloses nor suggests the use of such tables to perform encryption or decryption. Applicant therefore respectfully submits that claim 15 and dependent claim 56 are not anticipated by Adams, Jr., and that the pending rejection of claims 15 and 56 should be reversed for this reason as well.

Independent claim 18 and dependent claim 21

Claim 18 is drawn to a system for decrypting data packets, in which each data packet intercepted (and potentially decrypted) includes an address header including broadcast addresses of the first computer and second computers (source and destination computers). As described above, Adams, Jr. through its disclosure of a system in which a gateway address is provided in a packet header does not anticipate the invention of claim 18 and therefore the pending rejection of claim 18 should be reversed for at least the reasons set forth.

Claim 21 depends from claim 18. Therefore, Adams, Jr. does not anticipate the invention of claim 21 and the pending rejection of claim 21 should be reversed for this reason as well.

Dependent claim 19

Claim 19 depends directly from independent claim 18 and further requires that the data packet includes the new data packet in encrypted form. In other words, the data packet is the decrypted data packet in encrypted form. Adams, Jr. in no manner discloses or suggests that the data packet having an address header including broadcast addresses of the first and second computers is also encrypted. Adams, Jr. therefore does not anticipate the invention of claim 19 and the pending rejection of claim 19 should be reversed for this reason as well.

Independent claim 22

Claim 22 is drawn to a method for receiving and decrypting data packets, in which a data packet is intercepted which includes an address header including broadcast addresses of the first and second computers (source and destination computers). As described above, Adams, Jr. through its disclosure of a system in which a gateway address is provided in a packet header does not anticipate the invention of claim 22 which provides broadcast addresses of the source and destination computers in the packet header.

In addition, claim 22 further requires that the body of the packet header includes address information representing an internetwork address of the first computer and an internetwork address of the second computer. Thus, rather than identifying an actual node in the header, the node is identified in the body of the packet. Adams, Jr. neither discloses nor suggests a method of receiving and decrypting data packets in which the address header includes broadcast addresses of the source and destination computers while the body includes the internetwork address of the source and destination computers. Adams, Jr. therefore does not anticipate the invention of claim 22 and the pending rejection of claim 22 should be reversed for at least the reasons set forth.

Dependent claim 23

Claim 23 directly depends from independent claim 22, and further requires that the body of the data packet includes the new data packet (i.e., the decrypted data packet), which includes a new address header, in encrypted form. Adams, Jr. neither discloses nor suggests a method of receiving and decrypting data packets in which the address header includes broadcast addresses of the source and destination computers, where the body of the data packet includes the new data

packet (including the new address header) in encrypted form. It is therefore respectfully submitted that Adams, Jr. neither teaches nor reasonably suggests the invention of claim 23, and therefore the pending rejection of claim 23 should be reversed for this reason as well.

Independent claims 32 and 33

Claims 32 and 33 are each drawn to a method of encrypting data packets producing a modified data packet including a header portion storing an identifier of a network. The network corresponds to the source of the data packet in claim 32, while the network corresponds to the destination of the data packet in claim 33.

Adams, Jr. discloses the specification of an address of a particular node in the packet header. More particularly, Adams, Jr. specifically requires that the gateway (CNEDD) address is be provided in the packet header. In contrast, the invention of each of claims 32 and 33 specifically requires that the header portion store an identifier of a network. In this manner, the present invention avoids providing the address of a gateway responsible for encryption and/or decryption of the data packet in the packet header, as disclosed by Adams, Jr. The system in Adams, Jr. is entirely susceptible to outsiders wishing to tap into the network, since such outsiders may easily ascertain the nodes responsible for encryption as well as decryption. The presently claimed invention therefore provides greater protection than Adams, Jr. against tapping into the network to decipher the nature of the information transmitted (e.g., via the gateway responsible for encryption or decryption).

In addition, claims 32 and 33 each further require that encrypting the data packet produces an encrypted data packet including an encrypted header section and an encrypted data section. In this manner, even greater protection against tapping into the network is afforded. Adams, Jr. neither discloses nor suggests encrypting a header that stores an identifier of a network. Therefore, it is respectfully submitted that claims 32 and 33 are not anticipated by Adams, Jr., and that the pending rejection of claims 32 and 33 should be reversed for at least the reasons set forth.

Independent claims 40, 50, and 52

Independent claims 40, 50, and 52 each pertain to a method, a computer program product, or a computer system for decrypting data packets. More specifically, each of claims 40, 50, and 52 specifically requires that a received data packet include a header section that stores a

destination identifier identifying a broadcast address of the destination of the data packet and a source identifier identifying a broadcast address of the source of the data packet. As described above with reference to independent claim 7, Adams, Jr. specifically requires that the gateway (CNEDD) address be provided in the packet header. However, in no manner does Adams, Jr. disclose storing broadcast addresses in the packet header.

Claims 40, 50, and 52 each further require that it be determined whether the data packet is encrypted upon reference to at least one of the source and destination identifiers. Adams, Jr. neither discloses nor suggests determining whether a data packet is encrypted based upon broadcast addresses of the source and destination which are provided in the packet header. Applicant therefore respectfully submits that claims 40, 50, and 52 are not anticipated by Adams, Jr., and that the pending rejection of these claims should be reversed for at least the reasons set forth.

Dependent claims 41-49, 51, and 53

Dependent claim 41 depends directly from claim 40 and further recites transmitting the decrypted data packet to the destination. Adams, Jr. neither discloses nor suggests transmitting a packet that has been decrypted once it has been determined that the packet is encrypted (based upon broadcast addresses of the source and destination as provided in the packet header). It is therefore respectfully submitted that claim 41 is not anticipated by Adams, Jr., and that the pending rejection of claim 41 should be reversed for this reason as well.

Dependent claim 42 depends directly from claim 40, and further recites wherein determining whether the data packet is encrypted comprises accessing stored information that indicates by presence or absence of the source identifier that data packets from the source are encrypted. Adams, Jr. neither discloses nor suggests accessing stored information that indicates by presence or absence of the source identifier (which identifies a broadcast address associated with the source) that data packets from the source are encrypted. It is therefore respectfully submitted that claim 42 is not anticipated by Adams, Jr., and that the pending rejection of claim 42 should be reversed for this reason as well.

Dependent claim 43 depends directly from claim 40, and further recites wherein determining whether the data packet is encrypted comprises accessing stored information that indicates by presence or absence of a correlation between the source and destination identifiers that data packets from the source for the destination are encrypted. Adams, Jr. neither discloses nor suggests accessing stored information that indicates by presence or absence of a correlation

between the source and destination identifiers (which are broadcast addresses) that data packets from the source for the destination are encrypted. It is therefore respectfully submitted that claim 43 is not anticipated by Adams, Jr., and that the pending rejection of claim 43 should be reversed for this reason as well.

Dependent claim 44 depends directly from claim 40, and further recites wherein the data section of the data packet includes an encrypted header section and an encrypted data section, the encrypted header section including a header of the decrypted data packet after encryption and the encrypted data section including a body of the decryped data packet after encryption. Adams, Jr. neither discloses nor suggests where the data packet has a header section of claim 40 and a data section that includes such an encrypted header section and encrypted data section. Therefore, it is respectfully submitted that claim 44 is not anticipated by Adams, Jr., and that the pending rejection of claim 44 should be reversed for this reason as well.

Dependent claims 45-49, 51, and 53 depend from one of independent claims 40, 50 and are therefore patentable over Adams, Jr. for at least the same reasons. However, the dependent claims recite additional limitations that further distinguish them from the cited references. Hence, it is submitted that dependent claims 45-49, 51, and 53 are patentably distinct from Adams, Jr.

Claims 40-43 and 44-53 pertain to decryption of a data packet including a header section that stores a destination identifier of a broadcast address of the destination of the data packet and a source identifier of a broadcast address of the source of the data packet. While claims 40-41 and 44-49 each pertain to a method of decrypting data packets, claims 50-51 each pertain to a computer program product for decrypting data packets and claims 52-53 each pertain to a computer system for decrypting data packets.

Claims 57-59

Claims 57 is drawn to a system for encrypting data packets in which a modified data packet including a new address header is generated. The claim specifically requires that the new address header include internetwork broadcast addresses of the first and second computer networks (corresponding to the source and destination of the data packet).

Claims 58 and 59 are drawn to a computer program product or computer system for encrypting data packets in which a modified data packet including a new address header is generated. The claim specifically requires that the new address header store at least one of a

broadcast address associated with the source and a broadcast address associated with the destination.

Applicant respectfully submits that Adams, Jr. neither discloses nor suggests a method of encrypting data packets in which a modified data packet includes a new address header including broadcast addresses associated with the source and destination of the data packet. Hence, it is submitted that dependent claims 57-59 are patentably distinct from Adams, Jr.

Adams, Jr. – claims 1-6, 9-13, 16-17, 20, 24-31, 34-39, 54-55, and 60-73

Claims 1-6, 9-13, 16-17, 20, 24-31, 34-39, 54-55, and 60-73 stand rejected as being anticipated by Adams, Jr. et al. The Examiner indicates that disclosure of a header indicating whether a data packet is encrypted and the number of padding bytes used in the encryption anticipates claims providing a mechanism for identifying an encryption/decryption method in a header of an encrypted data packet. Applicant respectfully traverses this assertion.

Claims 1, 6, 11, 16, and 17, as amended, are drawn to a method or system adapted for encrypting a data packet according to a predetermined encryption/decryption mechanism, generating a new header including a mechanism for identifying the predetermined encryption/decryption mechanism and appending the new header to the encrypted data packet.

Similarly, claims 20 and 24 are drawn to a method or system for decrypting a data packet including a header that includes a mechanism for identifying an encryption method used to encrypt the data packet.

Claim 54 is drawn to a system that includes instructions for encrypting a data packet, generating a new address header for the data packet and for appending an encapsulation header to the data packet. The encapsulation header includes the new address header and a mechanism for identifying a predetermined encryption/decryption mechanism used to encrypt the data packet.

Claim 60 is drawn to a method of decrypting data packets comprising receiving a data packet including a header section and a data section, and decrypting the data packet. The header section stores encryption information providing a mechanism for identifying an encryption method used to generate the data packet. Similarly, claim 64 is drawn to a computer program

product for decrypting data packets, comprising receiving a data packet including a header section storing encryption information wherein the encryption information includes a mechanism for identifying an encryption method used to generate the data packet. Claim 67 is similarly drawn to a computer system for decrypting data packets, comprising computer code that causes a processor to receive a data packet including a header section and a data section. When it is determined from the header section that the data packet is encrypted, the data packet is decrypted. The header section stores encryption information including a mechanism for identifying an encryption method used to generate the data packet.

Claims 26, 36, and 38, as amended, are drawn to a method, computer program product, or computer system adapted for encrypting data packets. When a data packet is encrypted, a new header is generated and appended to the encrypted data packet. The new header includes a mechanism for identifying an encryption method used to generate the encrypted data packet. For instance, the mechanism may (but does not need to) be a Security Parameters Index which specifies which "row" of a Security-Association Table a receiver should use to interpret the received packet. Thus, through the identification of an entry in a Security-Association Table, an encryption method used to generate the encrypted data packet may be identified. As a result, the presently claimed invention permits the encryption method to be tailored for each packet transmitted rather than requiring that the encryption method be specified statically (e.g., according to the source and/or destination of the packet).

The Examiner refers to Adams Jr. and states that indicating in the header whether the data packet is encrypted and the number of padding bytes used in the encryption identifies an encryption method. Applicant respectfully traverses this assertion. Col. 8, lines 5-14 state: "If DES encryption is used, the amount of information to be encrypted per packet must be in multiples of 8 bytes. That is, the length of data characters 70 must be either 8, 16, 32, etc. bytes long for the DES encryption to be performed properly. If the amount of information to be encrypted is not a multiple of 8 bytes, "padding" bytes are added to increase the length of the information block before encryption takes place. This use of padding bytes is well known to those skilled in the art." Adams Jr. neither discloses nor suggests that the indication of the number of padding bytes is used to identify an encryption method. As described above, the number of bytes in a packet may vary when DES encryption is used. Thus, Adams Jr. merely implies that DES decryption may be performed properly through the identification of the number of padding bytes in the header of the encrypted data packet. Only one encryption method, DES, is discussed. Moreover, it is important to note that a variety of encryption methods may also

require that the amount of information encrypted per packet be in multiples of 8 bytes long for the encryption to be performed properly, as described above with respect to DES encryption. Since there need not be a one-to-one correspondence between the encryption method and the number of padding bytes, the mere indication of the number of padding bytes cannot identify, either directly or indirectly, the encryption method used.

None of the cited references, separately or in combination, disclose or suggest a mechanism for identifying an encryption/decryption method in a header of the encrypted data packet. Similarly, none of the cited references disclose or suggest decrypting a data packet that has a header including a mechanism for identifying the encryption method used to encrypt the data packet. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejection of independent and dependent claims 1-6, 9-13, 16-17, 20, 24-31, 34-39, 54-55, and 60-73.

SUMMARY

Reconsideration of the application and an early Notice of Allowance are earnestly solicited. If there are any issues remaining which the Examiner believes could be resolved through either a Supplemental Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned attorney at the telephone number listed below.

Applicants hereby petition for an extension of time which may be required to maintain the pendency of this case, and any required fee for such extension or any further fee required in connection with the filing of this Amendment is to be charged to Deposit Account No. 50-0388 (Order No. SUN1P342R).

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

Elise R. Heilbrunn
Reg. No. 42,649

P.O. Box 778
Berkeley, CA 94704-0778